

EXHIBIT B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, et al.,
Plaintiffs,
v.
GOOGLE LLC,
Defendant.

Case No. 20-CV-05146-LHK

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS WITH LEAVE TO AMEND**

Re: Dkt. No. 57

Plaintiffs Patrick Calhoun, Elaine Crespo, Hadiyah Jackson, and Claudia Kindler (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, sue Defendant Google LLC (“Google”). Before the Court is Google’s motion to dismiss Plaintiffs’ complaint. ECF No. 57. Having considered the parties’ submissions and oral arguments, the relevant law, and the record in this case, the Court GRANTS IN PART AND DENIES IN PART Google’s motion to dismiss with leave to amend.

I. BACKGROUND

A. Factual Background

1. Google’s Alleged Collection of Plaintiffs’ Data

Plaintiffs are users of Google’s Chrome browser who allege that they “chose not to ‘Sync’

their [Chrome] browsers with their Google accounts while browsing the web . . . from July 27, 2016 to the present.” ECF No. 1 (“Compl.”) ¶ 1. Chrome’s Sync feature enables users to store their personal information by logging into Chrome with their Google account. *Id.* ¶ 39.¹

Plaintiffs allege that “Chrome sends . . . personal information to Google when a user exchanges communications with any website that includes Google surveillance source code . . . regardless of whether a user is logged-in to Google Sync or not.” *Id.* ¶ 134 (emphasis omitted). According to Plaintiffs, Google’s code “is found on websites accounting for more than half of all internet tracking” and “Chrome is . . . used on a majority [59%] of desktop computers in the United States, giving Google unprecedented power to surveil the lives of more than half of the online country in real time.” *Id.* ¶¶ 9, 194.

Plaintiffs allege Google collects five different types of personal information: (1) “The user’s unique, persistent cookie identifiers”; (2) “The user’s browsing history in the form of the contents of the users’ GET requests and information relating to the substance, purport, or meaning of the website’s portion of the communication with the user”; (3) “In many cases, the contents of the users’ POST communications”; (4) “The user’s IP address and User-Agent information about their device”; and (5) The user’s X-Client Data Header. *Id.* ¶ 134.

First, according to Plaintiffs, Google collects “[t]he user’s unique, persistent cookie identifiers.” *Id.* ¶ 134. “A cookie is a small text file that a web-server can place on a person’s web browser and computing device when that person’s web browser interacts with the website server.” *Id.* ¶ 55. According to Plaintiffs, “[c]ookies are designed to and, in fact, do operate as a means of identification for Internet users.” *Id.* ¶ 57. Plaintiffs allege that “Google uses several cookies to identify specific Internet users and their devices.” *Id.* ¶ 61. Plaintiffs further allege that “Google also engages in a controversial practice known as ‘cookie synching’ which further allows Google

¹ According to Google, “Chrome offers four modes: (1) Basic Browser; (2) Signed In; (3) Signed In with sync enabled; and (4) Incognito.” ECF No. 57 (“Mot.”) at 1 n.1. In the instant case, Plaintiffs allege that they used only the first two modes. *Id.* In a related case, *Brown v. Google*, the plaintiffs challenge Google’s data collection while they were in private browsing mode, which is called Incognito mode in Chrome. *See* Case No. 20-CV-03664-LHK, ECF No. 168, ¶ 11.

1 to associate cookies with specific individuals.” *Id.* ¶ 62.

2 Second, Plaintiffs allege that Google collects “[t]he user’s browsing history in the form of
3 the contents of the users’ GET requests and information relating to the substance, purport, or
4 meaning of the website’s portion of the communication with the user.” *Id.* ¶ 134. A GET request is
5 one of “[t]he basic commands that Chrome uses to send the users’ side of a communication.” *Id.* ¶
6 114. When a user types a website address or clicks a link to a website, “Chrome contacts the
7 website . . . and sends a [GET request].” *Id.* ¶ 115. According to Plaintiffs, Chrome “[p]laces the
8 contents of [a] GET . . . request in storage in the browser’s web-browsing history and short-term
9 memory.” *Id.* ¶ 117. Chrome allegedly stores the contents of the communication “so that, if the
10 user’s web-browser crashes unexpectedly, when the user re-starts their browser, the browser will
11 be able to offer the user the ability to return to their last communications prior to the browser’s
12 crash.” *Id.* ¶ 118.

13 Third, Plaintiffs allege that Google collects “[i]n many cases, the contents of the users’
14 POST communications.” *Id.* ¶ 134. Like a GET request, a POST request is one of “[t]he basic
15 commands that Chrome uses to send the users’ side of a communication.” *Id.* ¶ 114. “If . . . [a]
16 user were filling out a form on [a] website and clicks a button to submit the information in the
17 form, Chrome . . . makes [a] connection with the website server [and] . . . sends a ‘POST’ request
18 that includes the specific content that the user placed in the form.” *Id.* ¶ 116. According to
19 Plaintiffs, Chrome “[p]laces the contents of [a] . . . POST request in storage in the browser’s web-
20 browsing history and short-term memory.” *Id.* ¶ 117. Chrome allegedly stores the contents of the
21 communication “so that, if the user’s web-browser crashes unexpectedly, when the user re-starts
22 their browser, the browser will be able to offer the user the ability to return to their last
23 communications prior to the browser’s crash.” *Id.* ¶ 118.

24 Fourth, according to Plaintiffs, Google collects “[t]he user’s IP address and User-Agent
25 information about their device.” *Id.* ¶ 134. “An IP address is a number that identifies a computer
26 connected to the Internet.” *Id.* ¶ 47. “IP addresses of individual Internet users are used by Internet
27

1 service providers, websites, and tracking companies to facilitate and track Internet
 2 communications.” *Id.* ¶ 50. Plaintiffs allege that “Google tracks IP addresses associated with
 3 specific Internet users” and “associate[s] specific users with IP addresses.” *Id.* ¶¶ 51–52. Plaintiffs
 4 further allege that “[b]ecause Google collects the IP Address and user agent information together,
 5 Google can identify a user’s individual device even if more than one device shares the same IP
 6 address.” *Id.* ¶ 54.

7 Finally, Plaintiffs allege that Google collects the user’s X-Client Data Header. *Id.* ¶ 134.
 8 The X-Client Data Header “is an identifier that when combined with IP address and user-agent,
 9 uniquely identifies every individual download version of the Chrome browser.” *Id.* ¶ 69. Plaintiffs
 10 allege that, as of March 6, 2018, the X-Client Data Header “is sent from Chrome to Google every
 11 time users exchange an Internet communication, including when users log-in to their specific
 12 Google accounts, use Google services such as Google search or Google maps, and when Chrome
 13 users are neither signed-in to their Google accounts nor using any Google service.” *Id.* ¶ 70.

14 **2. Google’s Representations to Plaintiffs**

15 According to Plaintiffs, “Google expressly promises Chrome users that they ‘don’t need to
 16 provide any personal information to use Chrome,’ and that ‘[t]he personal information that
 17 Chrome stores won’t be sent to Google unless you choose to store that data in your Google
 18 Account by turning on sync[.]’” *Id.* ¶ 2. Conversely, Google contends that it explicitly disclosed
 19 the alleged data collection. Mot. at 3–5. Four documents are of particular relevance regarding
 20 Google’s representations to users: (1) Google’s Terms of Service; (2) Google’s Privacy Policy; (3)
 21 Chrome’s Terms of Service; and (4) Chrome’s Privacy Notice. The Court discusses each
 22 document in turn.

23 First, as of March 31, 2020, Google’s Terms of Service stated that the “Terms of Service
 24 help define Google’s relationship with you as you interact with our services.” Compl. Exh. 4.
 25 Google’s Terms of Service state that “[u]nderstanding these terms is important because, by using
 26 our services, you’re agreeing to these terms.” *Id.* Prior versions of Google’s Terms of Service
 27

made similar statements.

From April 14, 2014 until March 31, 2020, Google's Terms of Service invoked Google's Privacy Policy as follows: "You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular services." Compl. Exh. 2, 3. As of March 31, 2020, Google's Terms of Service explicitly excluded Google's Privacy Policy: "Besides these terms, we also publish a Privacy Policy. Although it's not part of these terms, we encourage you to read it to better understand how you can update, manage, export, and delete your information" Compl. Exh. 4.

Google's Terms of Service also invoke Google's service-specific terms and policies: "Next to each service, we also list additional terms and policies that apply to that particular service. The Terms of Service, additional terms, and policies define our relationship and mutual expectations as you use these services." *Id.*

Finally, Google's Terms of Service state that "California law will govern all disputes arising out of or relating to these terms, service-specific additional terms, or any related services, regardless of conflict of laws rules." Compl. Exh. 4.

Second, Google's Privacy Policy states: "[A]s you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy." Compl. Exh. 7. Google's Privacy Policy states:

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

Id.

Google's Privacy Policy in effect from June 28, 2016 to August 29, 2016 made the following disclosures regarding Google's collection of data from users:

We collect information about the services that you use and how you use them, like when you . . . visit a website that uses our advertising services, or view and interact with our ads and content.

This information includes: . . . device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number).

When you use our services or view content provided by Google, we automatically collect and store certain information in server logs, [including] details of how you used our service, such as your search queries . . . Internet protocol address . . . device event information such as . . . the date and time of your request and referral URL [and] cookies that may uniquely identify your browser or your Google Account.

Cookies and similar technologies.

We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookies, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.

Id. (emphasis omitted). Subsequent versions of Google’s Privacy Policy made similar disclosures.

Third, Chrome’s Terms of Service state the following: “By using Chrome or Chrome OS, you agree to the Google Terms of Service . . . and these Google Chrome and Chrome OS Additional Terms of Service.” Compl. Exh. 6.

Finally, the Chrome Privacy Notice invites users to “[l]earn how to control the information that’s collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device.” Compl. ¶ 37, Exhs. 17–33. The Chrome Privacy Notice states: “You don’t need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you’re using.” *Id.* The Chrome Privacy Notice then states that “Basic browser mode . . . stores information locally on your system. This information might include:” “Browsing history

information”; “Personal information and passwords”; and “Cookies or data from websites you visit.” *Id.* The Chrome Privacy Notice later states: “The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.” Compl. ¶ 38, Exhs. 28–33.²

B. Procedural History

On July 27, 2020, Plaintiffs filed the instant case against Google. Compl. Plaintiffs sought to represent a class of “all persons residing in the United States who used Google’s Chrome browser on or after July 27, 2016 without choosing to Sync with any Google account and whose personal information was collected by Google.” *Id.* ¶ 259.

Plaintiffs brought 16 claims: (1) unauthorized interception of electronic communications under the Wiretap Act; (2) unauthorized electronic communication service (“ECS”) disclosure under the Wiretap Act, 18 U.S.C. § 2510; (3) unauthorized access to stored ECS communications under the Stored Communications Act (“SCA”), 18 U.S.C. § 2701; (4) unauthorized disclosures of stored communications under the SCA, 18 U.S.C. § 2701; (5) violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631; (6) invasion of privacy; (7) intrusion upon seclusion; (8) breach of contract; (9) breach of the implied covenant of good faith and fair dealing; (10) quasi-contract (restitution and unjust enrichment); (11) violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030(g); (12) violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; (13) statutory larceny, Cal. Penal Code §§ 484 and 496; (14) violation of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.*; (15) punitive damages under Cal. Civil Code § 3294; and (16) declaratory relief under 28 U.S.C. § 2201(a). *Id.* ¶¶ 266–426.

² The previous versions of Chrome’s Privacy Notice made very similar statements. *See* Compl. ¶ 38, Exhs. 17–24 (“The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google Account by signing into Chrome. Signing in enables Chrome’s synchronization feature.”); Compl. ¶ 38, Exhs. 25–27 (“The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google Account by turning on Chrome sync.”).

On September 18, 2020, the Court directed the parties to select 10 claims to litigate. ECF No. 51. On September 25, 2020, the parties selected the following 10 claims: (1) unauthorized disclosure under the Wiretap Act; (2) unauthorized access under the SCA; (3) unauthorized disclosures of stored communications under the SCA; (4) violation of the CIPA; (5) intrusion upon seclusion; (6) breach of contract; (7) breach of the implied covenant of good faith and fair dealing; (8) violation of the CFAA; (9) statutory larceny; and (10) violation of the UCL. ECF No. 54.

On October 5, 2020, Google filed the instant motion to dismiss, ECF No. 57 (Mot.), and a request for judicial notice, ECF No. 58. On November 9, 2020, Plaintiffs filed an opposition to Google's motion, ECF No. 67 ("Opp'n"), and their own request for judicial notice, ECF No. 66. On December 3, 2020, Google filed a reply in support of their motion to dismiss, ECF No. 81 ("Reply"), and a response to Plaintiffs' request for judicial notice, ECF No. 82.

The Court may take judicial notice of matters that are either "generally known within the trial court's territorial jurisdiction" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). However, to the extent any facts in documents subject to judicial notice are subject to reasonable dispute, the Court will not take judicial notice of those facts. *See Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001), *overruled on other grounds by Galbraith v. County of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002).

Plaintiffs request that the Court take judicial notice of an October 6, 2020 House Report; an October 13, 2011 Federal Trade Commission ("FTC") Order; and an August 8, 2012 FTC Complaint. ECF No. 66. The Court will take judicial notice of these documents as public records, which are proper subjects of judicial notice. *See, e.g., United States v. Black*, 482 F.3d 1035, 1041 (9th Cir. 2007).

Plaintiffs request that the Court take judicial notice of three publicly available Google webpages. ECF No. 66. Google requests that the Court take judicial notice of four versions of

Google’s Privacy Policy. ECF No. 58. These documents appear on publicly available websites and are thus proper subjects for judicial notice. *See, e.g., In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 813–14 (N.D. Cal. 2020) (taking judicial notice of Google’s Terms of Service, Privacy Policy, and a Google blog post); *Matera v. Google, Inc.*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (taking judicial notice of Google’s Terms of Service, “various versions of Google’s Privacy Policy,” and a Google webpage entitled “Updates: Privacy Policy”).

Google does not contest that the documents of which Plaintiffs request judicial notice are proper subjects of judicial notice. ECF No. 82. However, Google contends that Plaintiffs seek judicial notice of these documents for improper purposes. *Id.* Specifically, Google argues that the Court cannot take judicial notice of the October 6, 2020 House Report for the purpose of establishing that House investigators had the same understanding of Google’s Privacy Policy as Plaintiffs did. *Id.* at 1. Google further contends that the Court cannot take judicial notice of the FTC documents to show that Google is acting in bad faith. *Id.* at 2. Finally, Google argues that the Court cannot take judicial notice of the three publicly available webpages to show that Google knows that Google’s Privacy Policy is not sufficient for blanket consent. *Id.* at 4.

The Court agrees with Google that the Court cannot take judicial notice of any facts in these documents that are subject to reasonable dispute. *See Lee*, 250 F.3d at 689. Accordingly, to the extent any facts in these documents are subject to reasonable dispute, the Court will not take judicial notice of those facts. *Id.* Thus, the Court GRANTS Google’s request for judicial notice and GRANTS Plaintiffs’ request for judicial notice.

Finally, Plaintiffs move to file supplementary material, ECF No. 127, in response to arguments Google made about the Court’s website at the February 25, 2021 motion to dismiss hearing in a related case, *Brown v. Google* (“*Brown*”). *See* Case No. 20-CV-03664-LHK, Tr. of Feb. 25, 2021 Hearing at 47:13–16, ECF No. 104. Google never raised these arguments in their briefs on the motions to dismiss in either case or at the February 18, 2021 hearing on the instant motion to dismiss. The Court did not consider Google’s untimely arguments in the Court’s order

denying the motion to dismiss in the *Brown* case, ECF No. 113, and will not do so here. *See In re Apple Inc. Securities Litigation*, 2011 WL 1877988, *5 n. 6 (N.D. Cal. May 17, 2011) (“The Court is not inclined to consider this argument given that it was not briefed but rather was raised for the first time at the end of the hearing”); *White v. FedEx Corp.*, 2006 WL 618591, *2 (N.D. Cal. Mar. 13, 2006) (“The Court will not consider any arguments or evidence raised for the first time at the hearing”). Accordingly, the Court DENIES Plaintiffs’ motion to file supplementary material, ECF No. 127.

II. LEGAL STANDARD

A. Dismissal Pursuant to Federal Rule of Civil Procedure 12(b)(6)

Rule 8(a) of the Federal Rules of Civil Procedure requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). Rule 8(a) requires a plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

The Court, however, need not accept as true allegations contradicted by judicially noticeable facts, *see Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it “may look beyond the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the Court “assume the truth of legal conclusions merely because they are cast in

the form of factual allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere “conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Leave to Amend

If the Court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, “a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts.” *Id.* at 1130 (internal quotation marks omitted). Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d 522, 532 (9th Cir. 2008).

III. DISCUSSION

In its motion to dismiss, Google first contends that Plaintiffs’ claims should be dismissed because Plaintiffs and the websites consented to Google’s receipt of the data. Mot. at 8–11. Google later argues that Plaintiffs’ claims should be dismissed because of the statutes of limitations. Mot. at 25. Google also argues that Plaintiffs have failed to state nine of the ten selected claims for additional reasons. *Id.* at 11–25. The Court addresses in turn: (1) consent; (2) the statutes of limitations; and (3) Google’s other arguments for dismissal.

A. Consent

Google contends that (1) all claims should be dismissed because Plaintiffs consented to

Google's receipt of the data, and (2) Plaintiffs' unauthorized disclosure claims under the Wiretap Act and the SCA should be dismissed because the websites consented to Google's receipt of the data. *Id.* at 8–11. The Court addresses each argument in turn.

1. Google has not shown that Plaintiffs consented.

Consent is a defense to Plaintiffs' claims. *See* 18 U.S.C. § 2511(3)(b)(ii) (Wiretap Act) (stating that a communication may be divulged "with the lawful consent of the originator"); 18 U.S.C. § 2702(b)(3) (SCA unauthorized disclosure) (stating that a communication may be divulged with the "lawful consent of the originator"); *id.* § 2701(c)(2) (SCA unauthorized access) (providing an exception from liability for conduct authorized by the user); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955–56 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("Plaintiffs' consent . . . bars their common-law tort claims [for intrusion upon seclusion] . . ."); 18 U.S.C. § 1030(a)(5)(A) (CFAA) (prohibiting "the transmission of a program, information, code, or command . . . without authorization"); *People v. Brock*, 143 Cal. App. 4th 1266, 1274 (2006) ("Theft by larceny . . . is not committed when the property is taken with the owner's consent."); Cal. Pen. Code §§ 631(a), 632(a) (CIPA) (prohibiting wiretapping and eavesdropping "without the consent of all parties to the communication").³ Accordingly, Google contends that Plaintiffs consented to Google's alleged data collection. Mot. at 9.

"[A]s 'the party seeking the benefit of the exception,' it is Google's burden to prove consent." *Matera v. Google Inc.*, 2016 WL 5339806, at *17. Consent "can be explicit or implied, but any consent must be actual." *In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). In order for consent to be actual, the disclosures must "explicitly notify" users of the practice at issue. *Id.* at *13; *see also Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014) (explaining that, for a finding of consent, the disclosures must have given users

³ Consent is also a defense to Plaintiffs' breach of contract and good faith and fair dealing claims because if Plaintiffs consented to the alleged data collection, Google would not have breached its contract with Plaintiffs by engaging in the alleged data collection. Furthermore, consent is a defense to Plaintiffs' UCL claim, which is predicated on Google's representations and Plaintiffs' other claims. *See* Section III(C)(8), *infra*.

notice of the “specific practice” at issue). The disclosures must have only one plausible interpretation for a finding of consent. *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019) [hereinafter “*Facebook Consumer Profile*”]. “[I]f a reasonable . . . user could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct, then [the defendant] cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent).” *Id.* at 789–90.

In the instant motion, Google contends that users expressly consented to Google’s alleged data collection. Mot. at 9. In *In re Google, Inc.*, this Court rejected a similar argument made by Google. 2013 WL 5423918, at *12–*14. In that case, the plaintiffs alleged that Google had intercepted their email communications over Gmail, Google’s email service, in order to create user profiles and provide targeted advertising. *Id.* at *1. In Google’s motion to dismiss, Google contended that the plaintiffs expressly consented to the interception of their emails and pointed to its Terms of Service and Privacy Policies. *Id.* at *13. Analyzing these policies, the Court concluded that “[n]othing in the [p]olicies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google’s intent to engage in such interceptions.” *Id.* Accordingly, the Court found that “a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements.” *Id.*

In the instant case, Google contends that Plaintiffs “consented to Google’s [Terms of Service], which incorporated Google’s Privacy Policy.” Mot. at 9. Google further argues that Google’s Privacy Policy disclosed the alleged data collection:

We collect information about the services that you use and how you use them, like when you . . . visit a website that uses our advertising services, or view and interact with our ads and content.

This information includes: . . . device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number).

When you use our services or view content provided by Google, we automatically collect and store certain information in server logs, [including] details of how you used our service, such as your search queries . . . Internet protocol address . . . device event information such as . . . the date and time of your request and referral URL [and] cookies that may uniquely identify your browser or your Google Account.

Compl. Exh. 7.

However, the Court concludes that this general disclosure is insufficient for two reasons. First, Google contends that Plaintiffs “consented to Google’s [Terms of Service], which incorporated Google’s Privacy Policy.” Mot. at 9. However, as of March 31, 2020, Google’s Terms of Service explicitly excluded Google’s Privacy Policy: “Besides these terms, we also publish a Privacy Policy. *Although it’s not part of these terms*, we encourage you to read it to better understand how you can update, manage, export, and delete your information.” Compl. Exh. 4 (emphasis added). Thus, a reasonable user consenting to Google’s Terms of Service on or after March 31, 2020 might have concluded that she was not consenting to Google’s Privacy Policy.

Second, the Chrome Privacy Notice makes specific representations that could suggest to a reasonable user that Google would not engage in the alleged data collection. From April 14, 2014 until March 31, 2020, Google’s Terms of Service directed users to the additional terms for specific services, such as the Chrome Privacy Notice. *See* Compl. Exh. 2, 3 (“You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular services.”).

The Chrome Privacy Notice invites users to “[l]earn how to control the information that’s collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device.” Compl. ¶ 37, Exhs. 17–33. The Chrome Privacy Notice states: “*You don’t need to provide any personal information to use Chrome*, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you’re using.” *Id.* (emphasis added).

Furthermore, the Chrome Privacy Notice then states that “Basic browser mode . . . stores information locally on your system. This information might include:” “Browsing history

information”; “Personal information and passwords”; and “Cookies or data from websites you visit.” *Id.* The Chrome Privacy Notice later states: “*The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.*” Compl. ¶ 38, Exhs. 28–33 (emphasis added).

Based on these disclosures, a reasonable user could have concluded that he or she did not need to provide any personal information to use Chrome without sync. *See* Compl. ¶ 37, Exhs. 17–33 (“*You don’t need to provide any personal information to use Chrome*, but Chrome has different modes you can use to change or improve your browsing experience.”) (emphasis added). Moreover, a reasonable user could have concluded that using Chrome without sync was a way to control “the information that’s collected, stored, and shared when you use the Google Chrome browser.” *See id.* (stating that “[p]rivacy practices are different depending on the mode you’re using”). Specifically, a reasonable user could have concluded that if he or she used Chrome without sync, his or her personal information would not be sent to Google. *See* Compl. ¶ 38, Exhs. 28–33 (“The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.”).

Plaintiffs allege that these representations were misleading because Google collected Plaintiffs’ personal information when Plaintiffs used Chrome without sync. *Id.* ¶ 134. Specifically, Google collected “unique, persistent cookie identifiers”; “browsing history”; “POST communications”; the “user’s IP address and User-Agent information about their device”; and the user’s X-Client Data Header. *Id.* ¶ 134.

This data falls within the definition of personal information under California law, which governs Google’s Terms of Service. *See* Compl. Exh. 4. Indeed, California law defines personal information as “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” including “Internet or other electronic network activity information,” such as “browsing history, search history, and information regarding a consumer’s interaction with an

internet website, application, or advertisement.” Cal. Civ. Code § 1798.140. Moreover, Google’s own Privacy Policy defines personal information as “information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can reasonably be linked to such information by Google, such as information we associate with your Google account.” Compl. Exh. 16.⁴ As Google’s counsel conceded at the hearing on the instant motion, the data at issue in the instant case falls within these broad definitions of personal information. *See* Tr. of Feb. 18, 2021 Hearing at 51:24–52:1, 52:19, ECF No. 114.

In response, Google contends that Chrome’s Privacy Notice is accurate where it states that “*The personal information that Chrome stores* won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.” Compl. ¶ 38, Exhs. 28–33 (emphasis added). According to Google, readers would understand that “*the personal information that Chrome stores*” does not include “unique, persistent cookie identifiers”; “browsing history”; “POST communications”; the “user’s IP address and User-Agent information about their device”; and the user’s X-Client Data Header. *See* Reply at 2; Tr. of Feb. 18, 2021 Hearing at 30:12–16, 51:10–13, 53:3–19, ECF No. 114.

However, the Court finds Google’s argument unpersuasive because it is inconsistent with California state law, which governs Google’s agreement with users, and Google’s Privacy Policy. *See* Cal. Civ. Code § 1798.140 (defining personal information as “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” including “Internet or other electronic network activity information,” such as “browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement”); Compl. Exh. 16 (Google’s Privacy Policy) (defining personal information as “information that you provide to us which personally identifies you, such as your name, email

⁴ Even the Chrome Privacy Notice states that browsing history falls within the definition of “personal browsing data.” *See* Compl. Exhs. 18–23 (stating that personal browsing data can include browsing history).

address, or billing information, or other data that can reasonably be linked to such information by Google, such as information we associate with your Google account”). Accordingly, the Court concludes that a reasonable user could read Google’s representations to mean that, if the user was not synced, his or her browsing history, cookies, and site data would not be sent to Google.

In conclusion, the Court concludes that Google did not notify users that Google engages in the alleged data collection. To the contrary, Google’s representations might have led a reasonable user to believe that Google did not collect his or her personal information when the user was not synced. Accordingly, Google cannot show that Plaintiffs expressly consented to Google’s collection of data. *See In re Google*, 2013 WL 5423918, at *13 (rejecting Google’s argument that users expressly consented because Google did not notify users of the alleged interceptions).

2. Google has not shown that the websites consented.

Google next contends that Plaintiffs’ unauthorized disclosure claims under the Wiretap Act and the SCA should be dismissed because the websites consented to Google’s receipt of the data. Mot. at 9–11. The Wiretap Act and the SCA provide an exception to liability where an electronic communication service (“ECS”) divulges contents with the “lawful consent” of “the originator or an addressee or intended recipient of such communication.” *See* 18 U.S.C. §§ 2511(3)(b)(ii) (Wiretap Act); *id.* § 2702(b)(3) (SCA). Accordingly, Google argues that the websites lawfully consented to Google’s receipt of the data. Mot. at 9–11.

“[A]s ‘the party seeking the benefit of the exception,’ it is Google’s burden to prove consent.” *Matera v. Google Inc.*, 2016 WL 5339806, at *17. “Courts have cautioned that implied consent applies only in a narrow set of cases.” *In re Google*, 2013 WL 5423918, at *12 (rejecting Google’s argument that users had given implied consent, immunizing Google from liability under the Wiretap Act). “The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception.” *Id.* “Moreover, consent is not an all-or-nothing proposition.” *Id.* “Rather, ‘[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its

communications.” *Id.* (quoting *In re Phmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003)). “Thus, ‘a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.’” *Pharmatrak*, 329 F.3d at 19 (quotation omitted).

Google argues that the websites provided implied consent to Google’s interception. Mot at. 11. In making this argument, Google cites two twenty-year-old district court cases regarding DoubleClick (now known as Google Ad Manager), a service which was purchased by websites to gather users’ data for advertising purposes. *See Chance v. Avenue A*, 165 F. Supp. 2d 1153, 1160–62 (W.D. Wash. 2001); *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 509–11 (S.D.N.Y. 2001). Both district courts concluded that the websites impliedly consented to DoubleClick’s interception of their communications with users by installing DoubleClick’s code on their websites. *Id.* However, courts have distinguished these cases where “the circumstances permit no reasonable inference that the [entities] did consent.” *See, e.g., Pharmatrak*, 329 F.3d at 20.

Google contends that, like the websites in *In re DoubleClick* and *Avenue A*, the websites in the instant case provided implied consent to Google’s interception by installing Google’s code on their website. Mot at. 11. According to Plaintiffs, the presence of Google’s code on the website causes Plaintiffs’ browsers to send a duplicate GET request to Google’s servers. Compl. ¶¶ 122–23.

However, the Court concludes that Google has not met its burden to establish consent because, even assuming that Google has established that websites generally consented to the interception of their communications with users, Google does not demonstrate that websites consented to, or even knew about, the interception of their communications with users who were using Chrome without sync.

As the Court explained above, neither Google’s Privacy Policy nor any other disclosure to which Google points states that Google engages in the alleged data collection while users are using Chrome without sync. *See* Section III(A)(1), *supra*. To the contrary, Google’s disclosures state that the data will not be sent to Google when users use Chrome without sync. *Id.*

Specifically, the Chrome Privacy Notice states: “*The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.*” Compl. ¶ 38, Exhs. 28–33 (emphasis added). The Chrome Privacy Notice also states: “*You don’t need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you’re using.*” *Id.* (emphasis added). Thus, Google has not established that websites consented to, or even knew about, the interception of the subset of their communications that are with users who use Chrome without sync. *See Pharmatrak*, 329 F.3d at 19 (explaining that “[a] party may consent to . . . the interception of only a subset of its communications”). Accordingly, Google cannot show implied consent on the part of the websites.

B. Statutes of Limitations

Google next argues that Plaintiffs’ complaint should be dismissed because each of Plaintiffs’ claims exceed the applicable statutes of limitations. Mot. at 23–25. “A claim may be dismissed under Rule 12(b)(6) on the ground that it is barred by the applicable statute of limitations only when ‘the running of the statute is apparent on the face of the complaint.’” *Von Saher v. Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 969 (9th Cir. 2010) (quoting *Huynh v. Chase Manhattan Bank*, 465 F.3d 992, 997 (9th Cir. 2006)). “[A] complaint cannot be dismissed unless it appears beyond doubt that the plaintiff can prove no set of facts that would establish the timeliness of the claim.” *Id.* (quoting *Supermail Cargo, Inc. v. United States*, 68 F.3d 1204, 1206 (9th Cir. 1995)).

Seven of the selected claims have a limitations period of between one and three years. Specifically, “[u]nder the CIPA, the applicable statute of limitations is one year.” *Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020). The statute of limitations for Plaintiffs’ Wiretap Act claim, SCA claims, CFAA claim, and intrusion upon seclusion claim is two years. *See* 18 U.S.C. § 2520(e) (stating that the Wiretap Act has a limitations period of “two years after the date upon which the claimant first has a reasonable opportunity to discover the violation” for

Wiretap Act claims); 18 U.S.C. § 2707(f) (stating that the SCA has a limitations period of “two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation”); 18 U.S.C. § 1030(g) (stating that the CFAA has a limitations period of two years from “the date of the act complained of or the date of the discovery of the damage”); Cal. Civ. Proc. Code § 335.1 (setting a two year limitations period, which applies to intrusion upon seclusion claims). The statute of limitations for Plaintiffs’ statutory larceny claim is three years. *See* Cal. Civ. Proc. Code § 338(c). The statute of limitations for Plaintiffs’ contract claims (i.e., breach of contract and breach of the implied covenant of good faith and fair dealing) and UCL claims is four years. *See* Cal. Civ. Proc. Code § 337(a) (setting a four year statute of limitations for contract claims); Cal. Bus. & Prof. Code § 17208 (setting a four year statute of limitations for UCL claims).

Google contends that, because Plaintiffs seek to represent a putative class of users who did not sync their accounts from July 27, 2016 to the present, the seven selected claims that have a statute of limitations of three years or less are time-barred. Mot. at 25. Google further argues that, for Plaintiffs’ remaining selected claims, to which a four year statute of limitation applies, “Plaintiffs must allege when the challenged conduct first occurred so the Court may determine when the claims accrued.” *Id.* The Court rejects Google’s argument because each violation triggers a separate statute of limitations, and Plaintiffs allege that violations took place in July 2020, shortly before Plaintiffs’ complaint was filed on July 27, 2020.

The Ninth Circuit and California Supreme Court have held that separate, recurring invasions of the same right each trigger their own separate statute of limitations. The Ninth Circuit has held that, for Wiretap Act claims, “each interception is a discrete violation” with its own statute of limitations. *Bliss v. CoreCivic, Inc.*, 978 F.3d 1144, 1148 (9th Cir. 2020). In coming to this conclusion, the Ninth Circuit relied on the Wiretap Act’s “multiple references to ‘communication’ in the singular,” which showed that there was “no textual basis for morphing what otherwise would be considered separate violations into a single violation because they flow

from a common practice or scheme.” *Id.* The Ninth Circuit’s reasoning applies to Plaintiffs’ other claims, which also refer to “communication” or “act” in the singular. *See* Cal. Penal Code §§ 631(a) (prohibiting the unauthorized interception of “any message, report or communication”); *id.* § 632(a) (prohibiting the interception of a “confidential communication”); Cal. Penal Code § 502(e)(5) (stating that the statute of limitations is three years from “the date of the act complained of, or the date of the discovery of the damage, whichever is later”). Furthermore, the California Supreme Court “ha[s] long settled that separate, recurring invasions of the same right can each trigger their own statute of limitations.” *Aryeh v. Canon Business Solutions, Inc.*, 292 P.3d 871, 880 (Cal. 2013).

Because Plaintiffs allege that Google engaged in interceptions of their communications shortly before filing their complaint, Plaintiffs’ claims are not barred by the statutes of limitations. Indeed, Plaintiffs allege that Google intercepted their communications in July 2020. Compl. ¶¶ 154, 168, 174, 180. Plaintiffs filed the instant case on July 27, 2020, well within any of the applicable statutes of limitations. *See* Compl. Thus, the Court DENIES Google’s motion to dismiss on the basis of the statutes of limitations.

C. Other Arguments for Dismissal

Finally, Google contends that Plaintiffs have failed to state nine of the ten selected claims for additional reasons. *Id.* at 11–25. The Court addresses in turn the following claims: (1) unauthorized disclosure under the Wiretap Act and the SCA; (2) unauthorized access under the SCA; (3) intrusion upon seclusion; (4) breach of contract; (5) breach of the implied covenant of good faith and fair dealing; (6) violation of the CFAA; (7) statutory larceny; and (8) violation of the UCL.

1. Plaintiffs have not stated a claim for unauthorized disclosure under the Wiretap Act or the SCA.

The Wiretap Act provides that “a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity.” 18 U.S.C. § 2511(3)(a). Similarly, the

SCA provides that “a person or entity providing an electronic communication service the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” *Id.* § 2702(a).

Plaintiffs allege that Chrome is an electronic communication service (“ECS”) that “intentionally divulged the contents of user communications with non-Google websites to Google while those user communications were in transmission on Chrome” and “in electronic storage by Chrome.” Compl. ¶¶ 289–90, 316–17. Google contends that Plaintiffs’ unauthorized disclosure claims should be dismissed because Plaintiffs fail to allege that Google divulged the contents of any communication to a third party. Mot. at 11–12, 16–17.

The Court agrees with Google. In the instant case, Plaintiffs allege that Chrome “is an ECS.” Compl. ¶¶ 289–90, 316–17. Because Chrome is a Google service,⁵ the “person or entity providing [the ECS]” is Google. 18 U.S.C. § 2511(3)(a), *id.* § 2702(a). The Wiretap Act and the SCA prohibit “the person or entity providing [the ECS]” from divulging the contents of any communication to any person or entity, but Plaintiffs do not allege that Google divulged the contents of any communication to a third party. Rather, Plaintiffs allege that Google divulged information to itself. Compl. ¶¶ 289–90, 316–17. Accordingly, Plaintiffs’ unauthorized disclosure claims under the Wiretap Act and the SCA fail.

Another court in this district recently rejected an unauthorized disclosure claim under the SCA for similar reasons. In *In re Google Assistant Privacy Litigation*, the plaintiffs alleged that another Google service, Google Assistant, disclosed audio or transcripts to Google. 457 F. Supp. 3d 797, 822 (N.D. Cal. 2020) [hereinafter “*Google Assistant*”]. The court concluded that the plaintiffs could not state an unauthorized disclosure claim under the SCA because the plaintiffs did not allege that Google had divulged the information to a third party, and “[Google’s] own use of Plaintiffs’ data for advertising purposes does not constitute an unlawful ‘disclosure.’” *Id.* The

⁵ Plaintiffs acknowledge that Chrome is a Google service. Indeed, Plaintiffs allege that Google’s Terms of Service were part of the contract between Plaintiffs and Google. Compl. ¶ 26, 351.

same reasoning requires dismissal of Plaintiffs' unauthorized disclosure claims in the instant case.

In response, Plaintiffs invoke the ordinary course of business exception to the Wiretap Act. Opp'n at 13. However, as Plaintiffs acknowledge, the ordinary course of business exception applies to interception claims under the Wiretap Act, not unauthorized disclosure claims. *See* 18 U.S.C. § 2510(5)(a)(ii) (precluding liability for interceptions under the Wiretap Act based on the use of "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business").

Unlike the interception provision of the Wiretap Act, the unauthorized disclosure provision of the Wiretap Act provides that "*a person or entity providing an [ECS] to the public* shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity." 18 U.S.C. § 2511(3)(a) (emphasis added). Google is the "person or entity providing [the] ECS" in the instant case, and Plaintiffs do not allege that Google divulged the contents of any communication to any third party. Thus, the Court GRANTS Google's motion to dismiss Plaintiffs' claims for unauthorized disclosure under the Wiretap Act and the SCA. The Court does so with leave to amend because (1) Plaintiffs have not had an opportunity to amend their complaint; (2) amendment would not be futile, unduly prejudice the opposing party, or cause undue delay; and (3) Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532; *Google Assistant*, 457 F. Supp. 3d at 823 (dismissing the plaintiffs' unauthorized disclosure claim with leave to amend).

2. Plaintiffs have not stated a claim for unauthorized access under the SCA.

The SCA provides a cause of action against a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents unauthorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a). To state a claim under 18 U.S.C. § 2701(a),

1 Plaintiffs must show that Defendants “(1) gained unauthorized access to a ‘facility’ where it (2)
2 accessed an electronic communication in ‘electronic storage.’” *In re Facebook, Inc. Internet*
3 *Tracking Litigation*, 956 F.3d 589, 608 (9th Cir. 2020) [hereinafter “*Facebook Tracking*”].

4 The Court concludes that Plaintiffs cannot state an SCA claim for two reasons. First,
5 Google is exempt from liability because Google is the entity providing Chrome. Second,
6 Plaintiffs’ personal computing devices are not facilities. The Court addresses each issue in turn.

7 First, the SCA provides an exception from liability for “conduct authorized . . . by the
8 person or entity providing” the alleged ECS. 18 U.S.C. § 2701(c)(1). Plaintiffs allege that Chrome
9 is an ECS. Compl. ¶ 303. However, Plaintiffs never allege who the person or entity providing the
10 ECS is. *Id.* ¶¶ 301–313. In the absence of an allegation by Plaintiffs, the Court concludes that
11 Google is the entity providing the ECS because Google provides the Chrome browser, which is a
12 Google service. *See* Section III(C)(1), *supra*. In the instant case, Google was the entity allegedly
13 collecting Plaintiffs’ data. Accordingly, Google, the entity providing the ECS, authorized the
14 alleged collection of data. Because the alleged misconduct was authorized by the entity providing
15 the ECS, Google is not subject to liability under the SCA’s unauthorized access provision. *See* 18
16 U.S.C. § 2701(c)(1).

17 Another court in this district came to a similar conclusion when plaintiffs brought an
18 unauthorized access claim under the SCA based on a new Google privacy policy that permitted
19 Google to collect and combine personal information collected from different Google services into
20 a single user profile. *See In re Google, Inc. Privacy Policy Litigation*, 2013 WL 6248499, at *12
21 (N.D. Cal. Dec. 3, 2013). The court concluded that the plaintiffs’ SCA unauthorized access claim
22 “borders on frivolous, considering the plain language of [Section 2701(c)] that exempts conduct
23 authorized ‘by the person or entity providing’” an ECS. *Id.* The court explained that, “[w]hatever
24 the propriety of Google’s actions, it plainly authorized actions that it took itself.” *Id.* The same
25 reasoning applies to Plaintiffs’ SCA claims in the instant case.

26 Second, Plaintiffs’ personal computing devices are not facilities. In the Complaint,
27
28

Plaintiffs point to four facilities: (1) Plaintiffs’ personal computing devices; (2) Plaintiffs’ Chrome browsers; (3) the browser-managed files which constitute all of the programs contained within Plaintiffs’ Chrome browsers; and (4) Plaintiffs’ IP addresses. *Id.* ¶ 307.

The SCA does not provide a statutory definition of facility. *Google Assistant*, 457 F. Supp. 3d at 820. However, the SCA specifies that a facility must be one “through which an [ECS] is provided.” 18 U.S.C. § 2701(a)(1). Based on this language, several “courts in this Circuit and others have interpreted ‘facility’ to exclude users’ personal devices.” *Google Assistant*, 457 F. Supp. 3d at 821. For example, the Fifth Circuit concluded that an individual’s personal device “does not provide an electronic communication service just because the device enables use of electronic communication services.” *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012). Similarly, the Third Circuit held that plaintiffs’ personal computers or browsers were not facilities under the SCA. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 147–48 (3d Cir. 2015) [hereinafter “*Google Cookie*”]. Moreover, although the Ninth Circuit has not explicitly addressed the question of whether a personal device constitutes a facility, the Ninth Circuit has stated that the SCA “covers access to electronic information stored in *third party* computers.” *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1104 (9th Cir. 2014) (emphasis added); *see also Facebook Tracking*, 956 F.3d at 609 n.10 (declining to address the question of whether users’ personal computers constituted facilities under the SCA).

This Court and several courts in this district have also concluded that a user’s personal device is not a facility under the SCA. *See Google Assistant*, 457 F. Supp. 3d at 821 (concluding that plaintiffs’ personal devices were not facilities under the SCA); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017) (concluding that plaintiffs’ browsers in which defendant allegedly placed cookies were not facilities under the SCA), *aff’d*, 956 F.3d 589 (9th Cir. 2020); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. 2012) (holding that plaintiffs’ iPhones were not facilities under the SCA).

The Court comes to the same conclusion about Plaintiffs’ personal devices in the instant

case. As this Court previously explained, interpreting personal devices as facilities would “render other parts of the [SCA] illogical.” *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1058; *accord Google Assistant*, 457 F. Supp. 3d at 822–23. For example, the SCA provides an exception from liability for access to facilities that is “authorized . . . by the person or entity providing” the alleged ECS. 18 U.S.C. § 2701(c)(1). Under this provision, an ECS provider such as Google could authorize third parties to access users’ personal computers. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1058 (“It would certainly seem odd that the provider of a communication service could grant access to one’s home computer to third parties, but that would be the result of [plaintiff’s] argument”) (quoting *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270–71 (N.D. Cal. 2001)).

Based on the two deficiencies explained above, the Court GRANTS Google’s motion to dismiss Plaintiffs’ unauthorized access claim under the SCA. The Court does so with leave to amend because (1) Plaintiffs have not had an opportunity to amend their complaint; (2) amendment would not be futile, unduly prejudice the opposing party, or cause undue delay; and (3) Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532; *Google Assistant*, 457 F. Supp. 3d at 822 (“Although the Court is skeptical that Plaintiffs will be able to articulate yet another theory of unlawful access to an electronic storage ‘facility’, the Court will nonetheless grant [leave to amend].”).

3. Plaintiffs have stated an intrusion upon seclusion claim.

“To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant ‘intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]’ and (2) the intrusion ‘occur[red] in a manner highly offensive to a reasonable person.’ *Facebook Tracking*, 956 F.3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). To consider this claim, courts generally “ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *Id.* The Court addresses each element in turn.

a. Plaintiffs have adequately alleged that they had a reasonable expectation of

privacy.

To meet the first element, the plaintiff must have had an “objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source.” *Shulman v. Group W. Prods., Inc.*, 18 Cal. 4th 200, 231 (1998). “[T]he relevant question here is whether a user would reasonably expect that [Google] would have access to the . . . data.” *Facebook Tracking*, 956 F.3d at 602.

In *Facebook Tracking*, the Ninth Circuit considered whether the plaintiffs, who were Facebook users, had adequately pleaded that they had a reasonable expectation of privacy. *Id.* at 602. Like the instant case, *Facebook Tracking* concerned GET requests that were sent from Facebook users’ browsers to Facebook after they had logged out of Facebook. *Id.* at 601. Like Google, Facebook allegedly received copies of GET requests that users sent to third-party websites because Facebook’s embedded code caused the users’ browses to generate copies of the GET requests and transmit them to Facebook. *Compare id.* at 607 with Compl. ¶¶ 122–23.

The Ninth Circuit concluded that the plaintiffs had adequately pleaded that they had a reasonable expectation of privacy based on the amount of data collected, the sensitivity of the data collected, the nature of the data collection, and Facebook’s representations to users. *Facebook Tracking*, 956 F.3d at 602. First, the Ninth Circuit concluded that “the amount of data allegedly collected was significant”; Plaintiffs alleged that “Facebook obtained a comprehensive browsing history of an individual.” *Id.* Additionally, the Ninth Circuit emphasized that some of the alleged data collected was sensitive, such as information about a user’s visits to sensitive websites. *Id.* Furthermore, the Ninth Circuit found it significant “[t]hat this amount of information can be easily collected without user knowledge.” *Id.* Finally, the Ninth Circuit examined Facebook’s representations to users. *Id.* According to the Ninth Circuit, “Facebook’s privacy disclosures at the time allegedly failed to acknowledge its tracking of logged-out users, suggesting that users’ information would not be tracked.” *Id.* Accordingly, “Plaintiffs . . . plausibly alleged that, upon reading Facebook’s statements in the applicable Data Use Policy, a user might assume that only logged-in user data would be collected.” *Id.*

Other cases have come to similar conclusions. For example, in *Google Cookie*, the Third Circuit considered whether the plaintiffs had stated an intrusion upon seclusion claim under California law based on Google’s alleged placement of cookies on the browsers of users who had enabled cookie blockers. 806 F.3d 125, 132, 149 (3d. Cir. 2015). The Third Circuit concluded that the plaintiffs had a reasonable expectation of privacy based on “how Google accomplished its tracking,” which involved “overriding the plaintiffs’ cookie blockers, while concurrently announcing in its Privacy Policy that internet users could ‘reset your browser to refuse all cookies.’” *Id.* at 151. Similarly, in *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit considered whether the plaintiffs had stated a claim for intrusion upon seclusion under New Jersey law when Nickelodeon placed cookies on users’ browsers despite promising that it would not collect information from the users of its website. 27 F.3d 262, 293–94 (3d. Cir. 2016). The Third Circuit held that users had a reasonable expectation of privacy when Nickelodeon promised that it would not collect information from users of its website, but then did. *Id.*

In the instant case, the Court concludes that Plaintiffs have adequately alleged that they had a reasonable expectation of privacy in the data allegedly collected for two reasons. First, the amount of data collected, the sensitivity of the data collected, and the nature of the data collection demonstrate that Plaintiffs have a reasonable expectation of privacy. Second, based on Google’s representations, Plaintiffs could have reasonably assumed that Google would not receive their data while they were not synced. The Court discusses each reason in turn.

First, Plaintiffs have adequately alleged that they had a reasonable expectation of privacy based on the amount of data collected, the sensitivity of the data collected, and the nature of the data collection. Indeed, as explained above, the instant case involves the same data and the same process by which the data was collected as *Facebook Tracking*. Compare *id.* at 607 (describing how Facebook’s code directs the user’s browser to copy the referrer header and sends a duplicate request to Facebook) with Compl. ¶ 122 (describing how Google’s code directs the user’s browser to send a duplicate request to Google). Like in *Facebook Tracking*, the amount of data collected

and the nature of the data collection demonstrate that Plaintiffs had a reasonable expectation of privacy. Like in *Facebook Tracking*, Plaintiffs allege that the amount of data collected was vast. *See* Compl. ¶ 122 (alleging that “up to 86 percent of popular websites” use Google’s code). Finally, like in *Facebook Tracking*, Plaintiffs allege that a vast amount of data was collected secretly, without any notice to users. *Id.* ¶ 5 (alleging that “Chrome secretly sends personal information to Google even when a Chrome user does not Sync”).

Second, like the plaintiffs in *Facebook Tracking*, Plaintiffs in the instant case could have reasonably assumed that Google would not receive their data while they were using Chrome without sync based on Google’s representations. *See* Section III(A)(1), *supra*. Accordingly, the Court concludes that Plaintiffs have adequately alleged that they had a reasonable expectation of privacy.

b. Plaintiffs have adequately alleged that the alleged intrusion was highly offensive.

“Determining whether a defendant’s actions were ‘highly offensive to a reasonable person’ requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder’s motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.” *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 287). “While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy.” *Id.* (citing *Hernandez*, 47 Cal. 4th at 287).

In *Facebook Tracking*, the Ninth Circuit held that “[t]he ultimate question of whether Facebook’s tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage.” *Id.* Specifically, the Ninth Circuit concluded that “Plaintiffs’ allegations of surreptitious data collection when individuals were not using Facebook are sufficient to survive a dismissal motion on the issue” of whether the alleged intrusion was highly offensive. *Id.*

As explained above, Plaintiffs in this case allege that Google was surreptitiously collecting the same type of data through the same process that was at issue in *Facebook Tracking*. See Section III(C)(3)(a), *supra*. Moreover, as explained above, Google’s representations regarding Chrome’s sync function could have led users to assume that Google would not receive the personal information at issue in the instant case while they were not synced. See Section III(A)(1), *supra*.

Other than pointing to its disclosures, which the Court has already addressed, *supra* Section III(A)(1), Google also argues that its conduct is not “highly offensive” because its interceptions “served a legitimate commercial purpose.” Mot. at 19–20. However, whether an intrusion is highly offensive requires a holistic consideration of a multitude of factors, only one of which is the “countervailing interests . . . [that] render the intrusion inoffensive,” such as the intrusion’s commercial purpose. See *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 287). Recognizing this, some courts have concluded that plaintiffs had sufficiently alleged that similar intrusions to the one at issue in the instant case are highly offensive. See *id.* (holding that the plaintiffs had sufficiently alleged that Facebook’s collection of duplicate copies of GET requests from users who were signed out was highly offensive); *Google Cookie*, 806 F.3d at 150 (concluding that the plaintiffs had sufficiently alleged that Google’s practice of circumventing cookie blockers was highly offensive). Indeed, in *Google Cookie*, the Third Circuit rejected a similar argument by Google. 806 F.3d at 150. Although Google argued that “tracking cookies are routine,” the court concluded that “[b]ased on the pled facts, a reasonable factfinder could indeed deem Google’s conduct ‘highly offensive.’” *Id.* at 150–51. The Court comes to the same conclusion in the instant case.

Thus, Plaintiffs have alleged sufficient facts to prevail on the issues of whether they had a reasonable expectation of privacy and whether the intrusion was highly offensive. Accordingly, Plaintiffs have stated an intrusion upon seclusion claim. The Court DENIES Google’s motion to dismiss Plaintiffs’ intrusion upon seclusion claim.

4. Plaintiffs have stated a claim for breach of contract.

“In order to establish a contract breach, Plaintiffs must allege: (1) the existence of a contract with [Google], (2) their performance under that contract, (3) [Google] breached that contract, and (4) they suffered damages.” *Facebook Tracking*, 956 F.3d 589, 610 (9th Cir. 2020). Plaintiffs allege that their relationship with Google was governed by a contract consisting of three documents: (1) Google’s Terms of Service; (2) Chrome’s Terms of Service; and (3) Chrome’s Privacy Notice. Compl. ¶¶ 26, 351. Plaintiffs allege that this contract included a promise that Chrome would not share their personal information with Google while they were not synced. *Id.* ¶ 352. Plaintiffs allege that Google breached this contract by engaging in the alleged data collection while they were not synced. *Id.* ¶ 353.

Google argues that Plaintiffs have failed to state a breach of contract claim for three reasons. First, Google argues that Plaintiffs have failed to plausibly allege that Google breached any promise in the Chrome Privacy Notice. Mot. at 20. In support of this argument, Google cites *Google Assistant*, where another court in this district dismissed the plaintiffs’ breach of contract claim. 457 F. Supp. 3d at 833. That court rejected the claim because “in paraphrasing the relevant terms, Plaintiffs have altered them.” *Id.*

The Court concludes that Plaintiffs have not altered the contractual terms at issue in the instant case. As the Court explained above, *supra* Section III(A)(1), Chrome’s Privacy Notice stated: “You don’t need to provide any personal information to use Chrome.” Compl. ¶ 37, Exhs. 17–33. In addition, Chrome’s Privacy Notice stated that “the personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google account by turning on sync.” Compl. ¶ 38, Exhs. 28–33.⁶ As the Court explained above, *supra* Section III(A)(1), these promises could have led a reasonable user to conclude that, because they did not

⁶ The previous versions of Chrome’s Privacy Notice made very similar statements. *See* Compl. ¶ 38, Exhs. 17–24 (“The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google Account by signing into Chrome. Signing in enables Chrome’s synchronization feature.”); Compl. ¶ 38, Exhs. 25–27 (“The personal information that Chrome stores won’t be sent to Google unless you choose to store that data in your Google Account by turning on Chrome sync.”).

1 sync, Google would not receive their personal information.

2 Despite Google's promises, Plaintiffs allege that "Google intentionally and unlawfully
3 causes Chrome to record and send users' personal information to Google regardless of whether a
4 user elects to Sync or even has a Google account." *Id.* ¶ 3. The information sent includes: "IP
5 addresses linked to user agents"; "[u]nique, persistent cookie identifiers including the Client ID";
6 "[u]nique browser identifiers called X-Client Data Headers"; and "[b]rowsing history." *Id.* ¶ 4. All
7 of this identifying information falls within the definition of personal information under California
8 law, which governs Google's Terms of Service, and under Google's Privacy Policy. *See* Cal. Civ.
9 Code § 1798.140 (defining personal information as "information that identifies, relates to,
10 describes, is reasonably capable of being associated with, or could reasonably be linked, directly
11 or indirectly, with a particular consumer or household," including "Internet or other electronic
12 network activity information," such as "browsing history, search history, and information
13 regarding a consumer's interaction with an internet website, application, or advertisement");
14 Compl. Exh. 16 (defining personal information as "information that you provide to us which
15 personally identifies you, such as your name, email address, or billing information, or other data
16 that can reasonably be linked to such information by Google, such as information we associate
17 with your Google account").

18 Second, Google contends that Plaintiffs cannot state a claim because Plaintiffs
19 "simultaneously claim that Google's receipt of the Data constituted a breach of contract when they
20 'agreed to share' the Data with Google as a form of consideration." Mot. at 20; *see also* Compl. ¶
21 356 (alleging that "Plaintiffs and other Un-Synched Chrome users also did not receive the benefit
22 of the bargain . . . for which they paid valuable consideration in the form of the [personal
23 information] they agreed to share"). However, just because Plaintiffs decided to share some of
24 their personal information does not mean that they agreed to share all of their personal
25 information. *See In re Google*, 2013 WL 5423918, at *14 (holding that consumers may consent to
26 some data collection and reject others). Accordingly, the Court rejects Google's argument.

1 Finally, Google argues that Google did not make promises but rather provided information
 2 in Chrome's Privacy Notice. Mot. at 20. In support of this argument, Google cites *Facebook*
 3 *Tracking*, where the Ninth Circuit concluded that an alleged breach of Facebook's "Privacy and
 4 Data Use Policies" was not a cognizable breach of contract because the policies "provide
 5 information—not commitments—regarding [the defendant's] use of information and how users
 6 can control that information" but do "not require the user to make any commitment." 956 F.3d at
 7 610.

8 However, the Court concludes that the instant case is distinguishable because the
 9 documents involved in the instant case did make commitments, rather than just providing
 10 information. First, Google's Terms of Service is the contract between the users and Google.
 11 Google's Terms of Service stated that the "Terms of Service help define Google's relationship
 12 with you as you interact with our services." Compl. Exh. 4. Google's Terms of Service state that
 13 "[u]nderstanding these terms is important because, by using our services, you're agreeing to
 14 these terms." *Id.*

15 Furthermore, Google's Terms of Service explicitly incorporated the additional terms,
 16 including the Chrome Privacy Notice, into the contract between the users and Google. From April
 17 14, 2014 until March 31, 2020, Google's Terms of Service invoked additional terms as follows:
 18 "Our Services are very diverse, so sometimes additional terms or product requirements . . . may
 19 apply . . . [T]hose additional terms become part of your agreement with us if you use those
 20 services." Compl. Exhs. 2, 3. The most recent version of Google's Terms of Service directs users
 21 to "[f]ollow these terms and service-specific additional terms" and state that where there is a
 22 conflict between Google's Terms of Service and "service-specific additional terms," the latter
 23 terms will govern. Compl. Exh. 4. This language demonstrates that, rather than being an
 24 informational resource, the Chrome Privacy Notice is part of the contract between Plaintiffs and
 25 Google. Thus, Plaintiffs have adequately pled a breach of contract claim. Accordingly, the Court
 26 DENIES Google's motion to dismiss Plaintiffs' breach of contract claim.

27 **5. Plaintiffs have stated a claim for breach of the implied covenant of good faith and**

fair dealing.

As to Plaintiffs' claim for breach of the implied duty of good faith and fair dealing, Google argues that the claim should be dismissed because it does not go beyond the breach of contract theories that Plaintiffs assert. Mot. at 21. In *Facebook Tracking*, the Ninth Circuit affirmed the district court's dismissal of the plaintiffs' claim for breach of the implied covenant of good faith and fair dealing because "as pleaded, the allegations did not go beyond the breach of contract theories asserted by Plaintiffs and were thus properly dismissed." 956 F.3d at 611 (citing *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990)).

However, when the allegations go beyond the breach of contract theories, courts have concluded that the plaintiffs have stated a breach of contract claim and a breach of the implied covenant of good faith and fair dealing claim. *See, e.g., Facebook Consumer Profile*, 402 F. Supp. 3d at 802 (noting that plaintiffs could state claims for breach of contract and breach of the implied covenant of good faith and fair dealing when the defendant makes a material modification to the contract without providing notice); *In re Easysaver Rewards Litig.*, 737 F. Supp. 2d 1159, 1174 (S.D. Cal. 2010) (denying motion to dismiss breach of implied covenant claim where the defendant not only violated the contract but also frustrated its purpose by sharing consumer information).

The instant case is distinguishable from *Facebook Tracking* because Plaintiffs' allegations go beyond the breach of contract theories that they assert. Plaintiffs allege not only that Google violated the contract between the parties, but also that Google acted in bad faith, such as by circumventing cookie blockers. *See, e.g., Compl.* ¶¶ 62–86. Thus, Plaintiffs have adequately pled a claim for breach of the implied covenant of good faith and fair dealing. Accordingly, the Court DENIES Google's motion to dismiss Plaintiffs' breach of the implied covenant of good faith and fair dealing claim.

6. Plaintiffs have not stated a CFAA claim.

The CFAA is an anti-hacking statute that creates liability for "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct,

intentionally caus[ing] damage without authorization, to a protected computer.” 18 U.S.C. § 1030(a)(5)(A)(i). “Under the CFAA, Plaintiffs must . . . plead that [Google’s] actions caused loss of more than \$5,000 during any one-year period.” *Brodsky v. Apple, Inc.*, 2019 WL 4141936, at *7 (N.D. Cal. Aug. 30, 2019). Plaintiffs may aggregate losses from multiple violations over the one-year period to meet the \$5,000 requirement. *Creative Computing v. GetLoaded.com LLC*, 386 F.3d 930 (9th Cir. 2004).

Google contends that Plaintiffs fail to allege that Google’s conduct caused them to experience a loss of more than \$5,000 during a one-year period. Mot. at 22. The Court agrees. As Plaintiffs conceded during the hearing on the instant motion, the Complaint never alleges that Plaintiffs suffered losses exceeding \$5,000 during a one-year period. *See* Compl. ¶¶ 372–381 (failing to allege that Plaintiff suffered losses exceeding \$5,000 during a one-year period); Tr. of Feb. 25, 2021 Hearing at 18:3–5, ECF No. 114 (“[W]e did not have an allegation specifically saying that losses would exceed \$5,000.”); *id.* at 18:10–12 (“There is no sentence in the complaint, which we acknowledge that says that -- that alleges that losses exceed \$5,000.”). Thus, the Court GRANTS Google’s motion to dismiss Plaintiffs’ CFAA claims. The Court does so with leave to amend because (1) Plaintiffs have not had an opportunity to amend their complaint; (2) amendment would not be futile,⁷ unduly prejudice the opposing party, or cause undue delay; and (3) Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

7. Plaintiffs have stated a statutory larceny claim.

California Penal Code Section 484 forbids theft, which includes obtaining property “by . . . false . . . representation or pretense.” Cal. Penal Code § 484. California Penal Code Section 496(a) prohibits the obtaining of property “in any manner constituting theft.” Cal. Penal Code § 496(a).

⁷ The Court notes that, in *Andrews v Sirius XM Radio*, the Ninth Circuit recently rejected a CFAA claim where the plaintiff alleged that he had suffered the requisite loss under the CFAA because the defendant “allegedly ‘stole [his] personal information without compensating [him].’” 932 F.3d 1253, 1262 (9th Cir. 2019). The Ninth Circuit concluded that the CFAA had “a narrow conception of ‘loss,’ and the definition does not include a provision that aligns with [the plaintiff’s] theory.” *Id.* Because Plaintiffs in the instant case never alleged that they suffered loss, the Court cannot evaluate whether Andrews precludes Plaintiffs’ theory of loss.

1 Plaintiffs allege that Google violated these sections by stealing Plaintiffs’ personal information
2 without Plaintiffs’ consent. Compl. ¶¶ 394–403.

3 Google argues that Plaintiffs cannot plead a statutory larceny claim for two reasons. First,
4 Google argues that the personal information that Google allegedly stole is not property. Mot. at
5 22. In support of this argument, Google cites this Court’s 2012 decision in *Low v. LinkedIn*
6 *Corporation*, which dismissed Plaintiffs’ conversion claim based on LinkedIn’s alleged
7 “exercise[] [of] dominion” over Plaintiffs’ personal browsing history and other personally
8 identifiable information because “the weight of authority holds that a plaintiff’s ‘personal
9 information’ does not constitute property.” 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012).

10 However, Google ignores this Court’s other rulings, both before and after *Low v. LinkedIn*
11 *In. See, e.g., Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 798–99 (N.D. Cal. 2011) (plaintiffs’
12 names were misappropriated and thus lost value which constituted an injury to plaintiffs); *In re*
13 *Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (plaintiffs’
14 personal information was stolen in a data breach and thus lost value which constituted an injury to
15 plaintiffs); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal.
16 Aug. 30, 2017) (same).

17 Similarly, courts have recognized the “growing trend across courts . . . to recognize the lost
18 property value” of personal information. *In re Marriott Int’l, Inc. Cust. Data Sec. Breach Litig.*,
19 440 F. Supp. 3d 447, 461 (D. Md. 2020) (concluding that personal information has value); *see also*
20 *In re Facebook Privacy Litigation*, 572 F. App’x 494, 494 (9th Cir. 2014) (holding that plaintiffs’
21 allegations that they were harmed by the dissemination of their personal information and by losing
22 the sales value of that information were sufficient to show damages for their breach of contract
23 and fraud claims).

24 Furthermore, California courts have also acknowledged that users have a property interest
25 in their personal information. *See CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860
26 (2006) (“A person’s identifying information is a valuable asset.”); *accord Facebook Tracking*, 956

F.3d at 600 (citing *Lepe* and holding that the plaintiffs had suffered economic injury after Facebook allegedly took their personal information in a similar process to that alleged here). Accordingly, Plaintiffs have adequately alleged that they were deprived of a property interest.

Second, Google argues that Plaintiffs cannot show that Google committed larceny. Mot. at 23. Specifically, Google argues that it did not take Plaintiffs' personal information, but rather made a copy, and thus there is no taking. *Id.* However, California courts have held that copying is theft because "although the owner may retain possession of the original property, there has been nevertheless a deprivation of property when a copy is made." *People v. Kwok*, 63 Cal. App. 4th 1236, 1249–50 (1998). Thus, Plaintiffs have adequately alleged a statutory larceny claim. Accordingly, the Court DENIES Google's motion to dismiss Plaintiffs' statutory larceny claim.

8. Plaintiffs have stated a UCL claim.

The UCL "provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent." *Backhaus v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1050 (N.D. Cal. 2014) (citing Cal. Bus. & Prof. Code § 17200).

Plaintiffs allege that Google violated all three prongs of the UCL. First, Plaintiffs allege that Google engaged in unlawful practices by violating federal and state statutes, including the SCA, CIPA, CFAA, and statutory larceny. Compl. ¶ 408. Second, Plaintiffs allege that Google engaged in unfair practices, including by violating federal and state statutes. *Id.* ¶ 410. Finally, Plaintiffs allege that Google engaged in fraudulent practices by assuring Plaintiffs that their personal information would not be sent to Google when they were not synced. *Id.* ¶ 412. Google contends that Plaintiffs' UCL claims fail for three reasons. Mot. at 23–25. The Court addresses each reason in turn.

First, Google argues that Plaintiffs lack statutory standing under the UCL because they fail to allege that Google caused them to lose "money or property." Mot. at 23–24. However, to satisfy the statutory standing requirement under the UCL, a plaintiff must merely suffer an injury in fact that is an "economic injury." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 321–22 (2011).

The Court concludes that Plaintiffs have met this requirement. Indeed, the Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing. *See In re Facebook Privacy Litigation*, 72 F. App'x 494, 494 (9th Cir. 2014) (concluding that the plaintiffs had plausibly alleged that they experienced harm when their personal information was disclosed in a data breach and they lost the sales value of their personal information); *In re Marriott Int'l, Inc. Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) (“[T]he growing trend across courts that have considered this issue is to recognize the lost property value of this information.”); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (holding that plaintiffs had adequately alleged injury in fact based on the loss of value of their personal information); *In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (concluding that the plaintiffs had plausibly alleged injury from the loss of value of their personal information).

Second, Google argues that Plaintiffs cannot show unlawful, unfair, or fraudulent conduct because the Complaint fails to allege that Google violated any of the laws on which the UCL claim is predicated. Mot. at 24–25. However, Plaintiffs have adequately pled their CIPA and statutory larceny claims, on which the UCL claim is predicated. *See* Compl. ¶ 408; Section III(C)(7), *supra*. In addition, Plaintiffs have adequately pled that Google engaged in fraudulent conduct by representing in the Chrome Privacy Notice that Plaintiffs’ personal information would not be shared. *See* Section III(A)(1), *supra*. Thus, Plaintiffs have stated a UCL claim.

Third, as to damages, Google argues that monetary damages are unavailable to Plaintiffs under the UCL. “The only monetary remedy available in a private action under the unfair competition law is restitution.” *Clark v. Superior Court*, 50 Cal. 4th 605, 613 (2010); *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1148 (2003) (holding that “nonrestitutionary disgorgement of profits is not an available remedy” under the UCL). Thus, the only monetary remedy Plaintiffs may seek is restitution.

Accordingly, the Court DENIES Google's motion to dismiss Plaintiffs' UCL claim.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS Google's motion to dismiss the following claims with leave to amend:

- Unauthorized disclosure under the Wiretap Act
- Unauthorized access under the SCA
- Unauthorized disclosure under the SCA
- CFAA

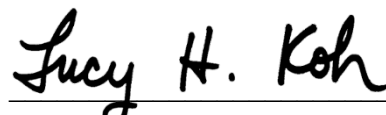
The Court DENIES Google's motion to dismiss the following claims:

- Breach of contract
- Breach of implied covenant of good faith and fair dealing
- Intrusion upon seclusion
- Statutory larceny
- UCL
- CIPA

Plaintiffs shall file any amended complaint within 30 days of this Order. Failure to do so, or failure to cure deficiencies identified herein or identified in the instant motion to dismiss, will result in dismissal of the deficient claims with prejudice. Plaintiffs may not add new causes of action or add new parties without stipulation or leave of the Court. Plaintiffs are directed to file a redlined complaint comparing the complaint to any amended complaint as an attachment to Plaintiffs' amended complaint.

IT IS SO ORDERED.

Dated: March 17, 2021



LUCY H. KOH
United States District Judge